UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/970,912	10/04/2001	Perry J. Robertson	SD-6769	3158

20567   7590   12/16/2004

SANDIA CORPORATION
P O BOX 5800
MS-0161
ALBUQUERQUE, NM 87185-0161

EXAMINER
SHIFERAW, ELENI A

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/970,912	ROBERTSON ET AL.
	Examiner	Art Unit
	Eleni A Shiferaw	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _04 October 2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-21_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-21_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _10/04/2001_.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-21 are presented for examination.

2.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.   Claims 1-5, and 12-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Takaragi et al. (Takaragi, US Patent Number: 4,969,190), in view of Johnson et al. (Johnson,

Patent Number 5,432,849).

As per claims 1 and 12, Takaragi teaches a method or a pipelined encryption/decryption engine

of enhancing throughput of a pipelined encryption/decryption engine for an

encryption/decryption process comprising a predetermined number of stages and

providing feedback around the stages, the method comprising the steps of:

indexing according to the encryption/decryption context identifier into a bank of initial

        receiving a source datablock for a given stage and encryption/decryption context

identifier (Takaragi Col. 4 lines 1-61; where i is identifier of each data block);

        indexing according to the encryption/decryption context identifier into a bank of initial

variables to retrieve an initial variable for the source datablock, the bank comprising a plurality

of initial variables for each encryption/decryption context identifier (Takaragi Col. 4 lines 39-

42); and

generating an output datablock from the source datablock and its corresponding initial variable (Takaragi Col. 4 lines 43-61).

Takaragi does not explicitly teach having plurality of initial vectors or variables,

However Johnston discloses set of predetermined control vectors C1,..., Cn (Johnston Col. 15 lines 54-67, and Fig. 11A).

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Johnston within the system of Takaragi because it would enhance security to data processing systems and methods and more particularly relates to cryptographic systems and methods for use in data processing systems (Johnston Col. 1 lines 10-14). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnston with in the system of Takaragi because it would allow a higher level of security.

As per claims 2 and 13, Takaragi and Johnston teach all the subject matter as described above. In addition Johnston teaches the method or the encryption/decryption engine, wherein in the indexing step/means the bank of initial variables comprises a number of initial variables for each encryption/decryption context identifier that is at least as large as the predetermined number of stages (Johnston Col. 15 lines 54-67, and Fig. 11A). The rational for combining are the same as claim 7 above.

As per claims 3 and 14, Takaragi and Johnston teach all the subject matter as described above. In addition, Takaragi teaches the method or the encryption/decryption engine, additionally comprising the step/means of replacing the corresponding initial variable with the output datablock (Takaragi Col. 3 lines 14-27).

As per claims 4, and 15, Takaragi and Johnston teach all the subject matter as described above. In addition, Takaragi teaches the method or the encryption/decryption engine, wherein the encryption/decryption process comprises Cipher Block Chaining Mode with exception of handling of initial variables (Takaragi Col. 2 lines 65-col. 3 lines 3).

As per claim 5, Takaragi and Johnston teach all the subject matter as described above. In addition, Takaragi teaches the method, wherein the encryption/decryption process comprises a block cipher capable of being pipelined (Takaragi Col. 3 lines 64-col. 4 lines 61).

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 6-11, and 16-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Takaragi et al. (Takaragi, US Patent Number: 4,969,190), in view of Johnson et al. (Johnson,

Patent Number 5,432,849), and in further view of Bruce Schneier (Schneier, Applied

Cryptography Second Edition, 1996).

As per claims 7 and 17, Takaragi teaches a method or an encryption/decryption engine for

enhancing throughput of a pipelined encryption/decryption engine for an encryption/decryption

process comprising a predetermined number of stages and providing feedback around the stages,

the method comprising the steps of:

means for, as to each of a plurality of encryption/decryption contexts, receiving a source

datablock for the corresponding encryption context identifier (Takaragi Col. 4 lines 1-25);

means for, as to for each of the plurality of encryption/decryption contexts, indexing

according to the encryption/decryption context identifier into a bank of variables comprising

initial variables (Takaragi Col. 4 lines 39-42) and prior-stage output datablocks to retrieve a seed

variable for the source datablock (Takaragi Col. 4 lines 39-61); and

means for, as to for each of the plurality of encryption/decryption contexts, generating an

output datablock from the source datablock and its corresponding seed variable (Takaragi Col. 4

lines 43-61);

wherein each stage of the pipelined encryption/decryption engine at any given time is

processing source datablocks from an encryption/decryption context different than

encryption/decryption contexts of source datablocks being processed in all other stages of the

pipelined encryption/decryption engine (Takaragi Col. 1 lines 31-50, col. 3 lines 59-63, and col.

4 lines 43-61),

Takaragi does not explicitly teach having plurality of initial vectors or variables,

However Johnston discloses set of predetermined control vectors C1,..., Cn (Johnston Col. 15 lines 54-67, and Fig. 11A).

However Johnston discloses set of predetermined control vectors C1,..., Cn (Johnston Col. 15 lines 54-67, and Fig. 11A) that reads on exceeding the predetermined number of stages or extra rounds of ciphering of blocks.

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Johnston within the system of Takaragi because it would enhance security to data processing systems and methods and more particularly relates to cryptographic systems and methods for use in data processing systems (Johnston Col. 1 lines 10-14). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Johnston with in the system of Takaragi because it would allow a higher level of security.

Takaragi and Johnston do not explicitly teach means for, as to each of a plurality of encryption/decryption contexts, a number of which equals or exceeds the predetermined number of stages,

However Schneier teaches means for, as to each of a plurality of encryption/decryption contexts, a number of which equals or exceeds the predetermined number of stages (Schneier Page 311par. 1, 2, and 3),

Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Schneier with in the combination system of Takaragi and Johnston because it would be more secure and difficult to break (Schneier Page 311 par. 1, 2, and 3).

As per claims 6, and 16, Takaragi, Johnson, and Schneier teach all the subject matter as described above. In addition Schneier teach the method, wherein the process is Digital Encryption Standard (DES) (Schneier Page 311 par. 5). The rational for combining are the same as claim 7 above.

As per claims 8 and 18, Takaragi, Johnson, and Schneier teach all the subject matter as described above. In addition, Takaragi teaches the method or the encryption/decryption engine, wherein each of the plurality of encryption/decryption contexts comprises a data stream to be encrypted (Takaragi Abstract; it is obvious that the data can be any kind of data including a telecommunication data).

As per claims 9, and 19, Takaragi, Johnson, and Schneier teach all the subject matter as described above. In addition Takaragi teaches the method, additionally comprising the step of decrypting the output datablocks at a plurality of locations distributed from the encryption/decryption engine corresponding in number to the number of encryption/decryption contexts (Takaragi Col. 4 lines 43-61).

As per claims 10, and 20, Takaragi, Johnson, and Schneier teach all the subject matter as described above. In addition, Takaragi teaches the method or the encryption/decryption engine, wherein the encryption/decryption process comprises Cipher Block Chaining Mode with exception of handling of initial variables (Takaragi Col. 2 lines 65-col. 3 lines 3).

As per claim 11, and 21 Takaragi, Johnson, and Schneier teach all the subject matter as described

above. In addition Schneier teaches the method wherein the encryption/decryption process

comprises a block cipher capable of being pipelined such as Digital Encryption Standard (DES).

(Schneier Page 311 par. 5). The rational for combining are the same as claim 7 above.

6.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Eleni A Shiferaw whose telephone number is 571-272-3867. The

examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

      If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

      Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
Art Unit 2136
December 6, 2004